Amendments to the Claims

1. (currently amended) A method for transmitting secured data over a wireless link ~~to a gateway providing access to a wide area network~~, the method comprising:

encrypting a payload according to a first session key ~~encryption algorithm~~;

adding a header to the encrypted payload to form a data packet;

encrypting the first session key;

encrypting ~~the encrypted payload and the forwarding header of~~ the data packet according to a second session key ~~encryption algorithm, the second encryption algorithm being an encryption algorithm used for secured communications over the wireless link, such that the data packet is decrypted according to the second encryption algorithm at the other end of the wireless link and prior to the gateway forwarding the data packet to the wide area network~~; ~~and~~

transmitting the encrypted first session key to a wireline device; and

transmitting the encrypted data packet over a ~~the~~ wireless link to a ~~the~~ gateway which decrypts the encrypted data packet, recreates the encrypted payload and the header, and forwards the encrypted payload and the header to the wireline device over an open network.

2. (currently amended) The method of claim 1, wherein the first session key ~~algorithm~~ uses a symmetric key.

3. (currently amended) The method of claim 1, further comprising:

receiving the encrypted first session key and the encrypted payload at the wireline device ~~data packet at the gateway~~;

decrypting the encrypted first session key~~data packet at the gateway according to the second algorithm~~; and

decrypting the encrypted payload using the decrypted first session key.

~~forwarding the recovered data packet to a computer on the wide area network; and~~

~~decrypting the payload at the computer on the wide area network according to the first algorithm.~~

4. (currently amended) The method of claim 1, wherein the ~~first~~ second session key ~~algorithm~~ uses a symmetric session key.

5. (canceled).

6. (currently amended) A device for transmitting data over a wireless link to a gateway providing access to a wide area network; comprising:

~~a wireless transceiver; and~~

an encryption engine ~~coupled to the wireless transceiver~~ which generates a first session key, encrypts ~~for encrypting~~ a payload according to a first session key~~encryption algorithm~~, adds ~~adding~~ a header to the payload to form a data

packet, encrypts the first session key; and encrypts ~~encrypting~~ the data packet according to a second session key~~encryption algorithm, the second encryption algorithm being an algorithm for secured communications over the wireless link, such that the data packet is decrypted according to the second encryption algorithm at the other end of the wireless link and prior to the gateway forwarding the data packet to the wide area network.~~; and

a wireless transceiver coupled to the encryption engine which transmits the encrypted first session key and transmits the encrypted data packet over a wireless link to a gateway which decrypts the encrypted data packet, recreates the encrypted payload and the header, and forwards the encrypted payload and the header to a server over an open network.

7. (canceled).

8. (currently amended) The device of claim 6, wherein the payload comprises location information regarding a ~~the~~ location of the wireless device.

9. (previously presented) The device of claim 6, wherein the first encryption algorithm employs a symmetric key.

10. (currently amended) A method for secured communication between a mobile device and a server on a wide area network, comprising:

~~generating a symmetric session key at the mobile device;~~

encrypting an unencrypted first ~~the symmetric~~ session key at the mobile device ~~using a public key associated with the server~~;

transmitting the encrypted first session key to the server over a wireless link ~~with a gateway to the wide area network~~;

decrypting the encrypted first session key at the server ~~using a private key corresponding to the public key~~;

encrypting a payload at the mobile device using the unencrypted first session key~~symmetric session key at the mobile device~~;

adding a header to the payload to form a data packet at the mobile device;

encrypting the ~~encrypted payload and the header of the~~ data packet according to a second session key configured ~~using an encryption algorithm~~ for secured communications over the wireless link ~~to form an encrypted data packet at the mobile device, the encryption data packet being so provided such that the data packet is decrypted according to the second encryption algorithm at the other end of the wireless link and prior to the gateway forwarding the data packet to the wide area network~~; and

transmitting the encrypted data packet from the mobile device to a ~~the~~ gateway which decrypts the encrypted data packet, recreates the encrypted payload and the header, and forwards the decrypted encrypted payload and the header to the server.

11. (currently amended) The method of claim 10, further comprising:

receiving the encrypted data packet at the gateway;

decrypting the encrypted data packet at the gateway to recover a decrypted data packet comprising ~~, the decrypted data packet having~~ the encrypted payload encrypted with the first ~~symmetric~~ session key;

forwarding the decrypted data packet to the server over the wide area network;

decrypting the encrypted first session key at the server using a private key; and

decrypting the encrypted payload at the server using the decrypted first session key.

12-14. (canceled).

15. (original) The method of claim 10, wherein the payload includes location information.

16. (currently amended) The method of claim 10, wherein the generating a first ~~symmetric~~ session key at the mobile device further comprises generating the first ~~symmetric~~ session key based on a random number.

17. (currently amended) The method of claim 10, wherein the encrypting a payload using the first ~~symmetric~~ session key employs at least one of the encryption algorithms DESX or DES.

18-19. (canceled).

20. (currently amended) The method of claim 1, wherein the first session key ~~algorithm comprises~~ implements at least one of the encryption algorithms DESX or DES.

21-24. (canceled).

25. (previously presented) The method of claim 1, wherein the data packet includes location information.

26. (currently amended) The method of claim 4, wherein the first ~~symmetric~~ session key is generated based on a random number.

27. (previously presented) The device of claim 6, further comprising a memory coupled to the encryption engine, the memory having a public key associated with a server on the wide area network stored therein.

28. (canceled).

29. (currently amended) A computer readable medium, comprising program instructions for performing a method comprising:

encrypting a payload according to a first session key~~encryption algorithm~~;

adding a header to the encrypted payload to form a data packet;

encrypting the first session key;

encrypting ~~the encrypted payload and the header of~~ the data packet according to a second session key~~encryption algorithm, the second encryption algorithm~~ configured ~~being an encryption algorithm used~~ for secured communications over a wireless link~~, such that the data packet is decrypted according to the second encryption algorithm at the other end of the wireless link and prior to the gateway forwarding the data packet to the wide area network~~; ~~and~~

transmitting the encrypted first session key to a server; and

transmitting the encrypted data packet ~~to a server on a wide area network~~ over a wireless link to ~~with~~ a gateway which decrypts the encrypted data packet, recreates the encrypted payload and the header, and forwards the encrypted payload and the header over an open network to the server which decrypts the encrypted first session key and decrypts the encrypted payload using the decrypted first session key~~providing access to the wide area network~~.

30. (currently amended) The computer readable medium of claim 29, wherein the first session key ~~algorithm~~ uses a symmetric key.

31. (currently amended) The computer readable medium of claim 29, the method further comprising:

receiving the data packet at the gateway;

decrypting the data packet at the gateway according to the second session key~~algorithm;~~

forwarding the encrypted payload to the server ~~recovered data packet to a computer on the wide area network; and~~

receiving the encrypted first session key at the server;

decrypting the encrypted first session key using a private key; and

decrypting the payload ~~at the computer on the wide area network~~ according to the first session key ~~algorithm~~.

32. (currently amended) The computer readable medium of claim 29, wherein the first session key ~~algorithm~~ uses a symmetric session key.

33. (previously presented) The computer readable medium of claim 29, wherein the first session key ~~algorithm~~ comprises at least one of the encryption algorithms DESX or DES.

34. (previously presented) The computer readable medium of claim 29, wherein the data packet includes location information.

35. (previously presented) The computer readable medium of claim 32, wherein the symmetric session key is generated based on a random number.